

SUBSTITUTE FORM PTO-1449
(MODIFIED)U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICEATTY. DOCKET NO.
10454/002001SERIAL NO.,
09/188,739INFORMATION DISCLOSURE
STATEMENT BY APPLICANT
(Use several sheets if necessary)

(37 CFR 1.98(b))

APPLICANT
Phillip A. Porras et al.FILING DATE
November 9, 1998

RECEIVED

JUL 25 1999
2182

U.S. PATENT DOCUMENTS

Group 2700

EXAMINER INITIAL		PATENT NUMBER							ISSUE DATE	PATENTEE	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
<i>JA</i>	AA	4	6	7	2	6	0	9	06/09/87	Humphrey et al.	371	21	03/28/86
<i>JA</i>	AB	4	7	7	3	0	2	8	09/20/88	Tallman	364	550	10/01/84
<i>JA</i>	AC	5	2	1	0	7	0	4	05/11/93	Husseiny	364	551.01	10/02/90
<i>JA</i>	AD	5	5	5	7	7	4	2	09/17/96	Smaha et al.	395	186	03/07/94
	AE												

FOREIGN PATENT OR PUBLISHED FOREIGN PATENT APPLICATION

		DOCUMENT NUMBER	PUBLICATION DATE	COUNTRY OR PATENT OFFICE	CLASS	SUBCLASS	TRANSLATION	
							YES	NO
	AF							
	AG							
	AH							
	AI							
	AJ							

OTHER DOCUMENTS (Including Author, Title, Date, Place of Publication)

<i>JA</i>	AK	Debar et al., "A Neural Network Component for an Intrusion Detection System," © 1992 IEEE						
<i>JA</i>	AL	Denning et al., "A Prototype IDIES: A Real-Time Intrusion-Detection Expert System," SRI Project ECU 7508, SRI International, MenloPark, California, August 1987						
<i>JA</i>	AM	Denning et al., "Requirements and Model For IDIES -- A Real-Time Intrusion-Detection Expert System," SRI Project 6169, SRI International, Menlo Park, CA, August 1985						
<i>JA</i>	AN	Denning, "An Intrusion-Detection Model," SRI International, Menlo Park, CA, Technical Report CSL-149, November 1985						
<i>JA</i>	AO	Dowell, "The Computerwatch Data Reduction Tool," AT&T Bell Laboratories, Whippany, New Jersey						
<i>JA</i>	AP	Fox et al., "A Neural Network Approach Towards Intrusion Detection," Harris Corporation, Government Information Systems Division, Melbourne, FL, July 2, 1990						
<i>JA</i>	AQ	Garvey et al., "Model-Based Intrusion Detection," Proceedings of the 14th National Computer Security Conference, Washington, DC, October 1991						

EXAMINER

DATE CONSIDERED

EXAMINER Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

SUBSTITUTE FORM PTO-1449
(MODIFIED)U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICEATTY. DOCKET NO.
10454/002001SERIAL NO..
09/188,739INFORMATION DISCLOSURE
STATEMENT BY APPLICANT
(Use several sheets if necessary)APPLICANT
Phillip A. Porras et al.FILING DATE
November 9, 1998GROUP
~~2762~~ 262

(37 CFR 1.98(b))

OTHER DOCUMENTS (Including Author, Title, Date, Place of Publication)

	BA	Ilgun et al., State Transition Analysis: A Rule-Based Intrusion Detection Approach, IEEE Transactions on Software Engineering, Vol. 21, No. 3, March 1995
	BB	Javitz et al., "The SRI IDES Statistical Anomaly Detector," Proceedings, 1991 IEEE Symposium on Security and Privacy, Oakland, California, May 1991
	BC	Liepins et al., "Anomaly Detection: Purpose and Framework," US DOE Office of Safeguards and Security
	BD	Lunt et al., "An Expert System to Classify and Sanitize Text," SRI International, Computer Science Laboratory, Menlo Park, CA
	BE	Lunt, "A Survey of Intrusion Detection Techniques," Computers & Security, 12 (1993) 405-418
	BF	Lunt, "Automated Audit Trail Analysis and Intrusion Detection: A Survey," Proceedings of the 11th National Computer Security Conference, Baltimore, MD, October 1988
	BG	Lunt et al, "Knowledge-Based Intrusion Detection"
	BH	Lunt et al., "A Prototype Real-Time Intrusion-Detection Expert System," Proceedings of the 1988 IEEE Symposium on Security and Privacy, April 1988
	BI	Porras et al., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, 20th NISSC -- October 9, 1997
	BJ	Porras et al., "Penetration State Transition Analysis A Rule-Based Intrusion Detection Approach, © 1992 IEEE
	BK	Sebring et al., "Expert Systems in Intrusion Detection: A Case Study
	BL	Shieh et al., "A Pattern-Oriented Intrusion-Detection Model and Its Applications © 1991 IEEE
	BM	Smaha, "Haystack: An Intrusion Detection System," © 1988 IEEE Computer Society Press: Proceedings of the Fourth Aerospace Computer Security Applications Conference, 1988, pp. 37-44
	BN	Snapp, "Signature Analysis and Communication Issues in a Distributed Intrusion Detection System," Thesis 1991

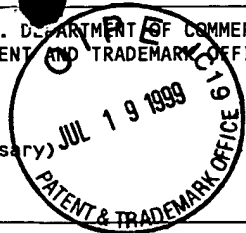
EXAMINER

DATE CONSIDERED

EXAMINER Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

SUBSTITUTE FORM PTO-1449
(MODIFIED)U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICEATTY. DOCKET NO.
10454/002001SERIAL NO.
09/188,739INFORMATION DISCLOSURE
STATEMENT BY APPLICANT
(Use several sheets if necessary)APPLICANT
Phillip A. Porras et al.FILING DATE
November 9, 1998GROUP
2762-2182

(37 CFR 1.98(b))



OTHER DOCUMENTS (Including Author, Title, Date, Place of Publication)

JA	CA	Snapp et al., "DIDS (Distributed Intrusion Detection System) -- Motivation, Architecture, and An Early Prototype, "Computer Security Laboratory, Division of Computer Science, Univ. of California, Davis, Davis, CA
		Tener, "AI & 4GL: Automated Detection and Investigation Tools," Computer Security in the Age of Information, Proceedings of the Fifth IFIP International Conference on Computer Security, W.J. Caelli (ed.)
JA	CB	Teng et al., "Adaptive Real-Time Anomaly Detection Using Inductively Generated Sequential Patterns,"
		© 1990
JA	CC	Vaccaro et al., "Detection of Anomalous Computer Session Activity," © 1989 IEEE
JA	CD	Weiss, "Analysis of Audit and Protocol Data using Methods from Artificial Intelligence," Siemens AG, Munich, West Germany
JA	CE	Winkler, "A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks," © Planning Research Corp. 1990
JA	CF	Jarvis et al., The NIDES Statistical Component Description and Justification, SRI International Annual Report A010, March 7, 1994
	CH	
	CI	
	CJ	
	CK	
	CL	
	CM	

EXAMINER

Thomas H. Hester

DATE CONSIDERED

4-5-01

EXAMINER: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.